LISTING OF CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (canceled)

2. (currently amended) ~~The system of claim 1, also~~ A repeater configured to implement a content protection protocol, for use in a communication system including~~:~~ a transmitter, an external agent configured to be coupled to the repeater and the transmitter, at least one transition minimized differential signaling-like ("TMDS-like") link coupled to the transmitter, a second TMDS-like link~~coupled to the receiver~~, and a receiver coupled to the second TMDS-like link and configured to receive re-encrypted data transmitted over the second TMDS-like link and to decrypt the re-encrypted data, wherein the transmitter is configured to implement the content protection protocol and is operable in an encryption mode to generate encrypted data using a secret value and transmit the encrypted data over the at least one TMDS-like link, the external agent is configured to respond to a ticket request by determining or obtaining a determination as to whether to grant the request, and to send signals to the transmitter and the repeater when coupled thereto in response to each granted ticket request to enable the transmitter and the repeater to operate respectively in the encryption mode and a decryption mode, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter and the repeater to obtain the secret value, and wherein the~~receiver is a~~ repeater includes:

first circuitry configured to be coupled to at least one said TMDS-like link to receive the encrypted data from the transmitter and configured to operate in the decryption mode in response to at least one of the signals sent by the external agent in response to said granted ticket request to generate decrypted data by decrypting the encrypted data using the secret value and to generate translated data by processing the decrypted data; and ~~,~~

second circuitry coupled to the first circuitry and configured to be coupled to the second TMDS-like link, wherein the second circuitry is configured to generate re-encrypted data by encrypting the translated data, and to transmit the re-encrypted data over the second TMDS-like link when coupled to said second TMDS-like link.~~; and~~

~~a second receiver coupled to the second TMDS-like link, wherein the second receiver~~

~~is configured to receive the re-encrypted data transmitted from the translating router and to decrypt the re-encrypted data~~ wherein the repeater is configured to send the ticket request to the external agent when the repeater is coupled to said external agent.

3. (canceled)

4. (canceled)

5. (currently amended) The repeater ~~system~~ of claim 88[[4]], wherein the repeater is configured to send a second ticket request to the external agent when the repeater is coupled to the external agent, and the external agent is configured to respond to the second ticket request by determining or obtaining a determination as to whether to grant the second ticket request, and sending second signals to the content source and the repeater in response to each granted second ticket request, wherein the second signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the content source and the repeater to obtain the second secret value.

6. (currently amended) The repeater ~~system~~ of claim 88[[4]], wherein the content protection protocol is an Advanced Encryption Standard ("AES") protocol and the second content protection protocol is ~~an~~ a High-bandwidth Digital Content Protection ("HDCP") protocol.

7. (currently amended) The repeater ~~system~~ of claim 88[[4]], wherein each of the content protection protocol and the second content protection protocol is an Advanced Encryption Standard ("AES") protocol.

8. (currently amended) The repeater ~~system~~ of claim 88[[4]], wherein the content protection protocol is a symmetric content protection protocol.

9. (currently amended) The repeater ~~system~~ of claim ~~1~~2, wherein the system also includes ~~including~~ a switch, wherein the at least one TMDS-like link includes a first TMDS-like link coupled between the transmitter and the switch, a ~~second~~third TMDS-like link coupled ~~between~~ to the switch ~~and the receiver~~, and a ~~third~~fourth TMDS-like link, wherein the switch is coupled to receive the encrypted data from the transmitter and to assert the

encrypted data over a selected one of the ~~second~~fourth TMDS-like link and the third TMDS-like link, and the first circuitry is configured to be coupled to the third TMDS-like link.

10. (canceled)

11. (canceled)

12. (canceled)

13. (currently amended) The router ~~system~~ of claim 90~~12~~, wherein the second secret value is identical to the third secret value.

14. (currently amended) The router ~~system~~ of claim 90~~12~~, wherein the at least one additional serial link is a transition minimized differential signaling-like ("TMDS-like") link ~~coupled between the router and the receiver~~.

15. (canceled)

16. (canceled)

17. (currently amended) The ~~system~~ translating router of claim 91~~16~~, wherein the translating router is configured to send a ticket request to the external agent when the translating router is coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to the translating router and the transmitter in response to each granted request, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the translating router and the transmitter to obtain the secret value.

18. (canceled)

19. (canceled)

20. (currently amended) The ~~system~~ translating router of claim 91~~16~~, wherein each of

the content protection protocol and the second content protection protocol is a symmetric content protection protocol.

21. (canceled)

22. (currently amended) The repeater ~~system~~ of claim 92~~21~~, wherein the repeater is configured to send a ticket request to the external agent when the repeater is coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to the repeater and the transmitter in response to each granted request, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the repeater and the transmitter to obtain the secret value.

23. (canceled)

24. (canceled)

25. (currently amended) The repeater ~~system~~ of claim 92~~21~~, wherein the repeater is configured to send a ticket request to the external agent when the repeater is coupled to the external agent, wherein the request is on behalf of the repeater and the receiver, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to at least one of the repeater and the receiver in response to each granted request, wherein the signals include at least one of the secret value and the second secret value, encrypted versions of the secret value and the second secret value, and data enabling the repeater to obtain the secret value and the second secret value and the receiver to obtain the second secret value.

26. (currently amended) The repeater ~~system~~ of claim 92~~21~~, wherein the second content protection protocol is a symmetric content protection protocol.

27. (currently amended) The repeater ~~system~~ of claim 26, wherein the second link is a TMDS-like link, the content protection protocol is an Advanced Encryption Standard ("AES") protocol and the symmetric content protection protocol is ~~an~~ a High-bandwidth Digital Content Protection ("HDCP") protocol.

28. (currently amended) The repeater ~~system~~ of claim 26, wherein the second link is a TMDS-like link, and the symmetric content protection protocol is a modified High-bandwidth Digital Content Protection ("HDCP") protocol which requires that the repeater and the receiver obtain the second secret value directly or indirectly from the external agent.

29. (currently amended) The repeater ~~system~~ of claim 92~~21~~, wherein the second link is a TMDS-like link, and each of the content protection protocol and the second content protection protocol is an Advanced Encryption Standard ("AES") protocol.

30. (currently amended) The repeater ~~system~~ of claim 29, wherein the second content protection protocol is an AES-128 CTR protocol, which is a counter mode of an AES-128 protocol.

31. (canceled)

32. (currently amended) The receiver ~~system~~ of claim 93~~31~~, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter and the receiver to obtain the secret value.

33. (currently amended) The receiver ~~system~~ of claim 93~~31~~, wherein the data indicative of at least one capability of the receiver indicates whether the receiver can assert unprotected digital data at an output of said receiver.

34. (currently amended) The receiver ~~system~~ of claim 93~~31~~, wherein the data indicative of at least one capability of the receiver indicates whether the receiver can assert digital data protected by a content protection protocol at an output of said receiver.

35. (canceled)

36. (canceled)

37-52. (canceled)

53. (canceled)

54. (currently amended) The agent ~~system~~ of claim 97~~53~~, wherein the code value is a key sequence code value.

55. (canceled)

56. (currently amended) The agent ~~system~~ of claim 97~~53~~, wherein the content protection protocol is a symmetric content protection protocol.

57. (canceled)

58-69. (canceled)

70. (canceled)

71. (currently amended) The receiver ~~system~~ of claim 99~~70~~, wherein the first data is a pseudo-random value, and the receiver is configured to generate the pseudo-random value for use in generating the authentication message.

72. (currently amended) The receiver ~~system~~ of claim 99~~70~~, wherein the receiver is configured to treat the receiver key as an invalid key unless the decrypted result satisfies the predetermined criterion.

73. (canceled)

74. (canceled)

75. (currently amended) The receiver ~~system~~ of claim 99~~70~~, also including a transition minimized differential signaling-like ("TMDS-like") link coupled to ~~between~~ the transmitter

~~and the receiver~~, wherein the receiver is configured to be coupled to the TMDS-like link, the protocol is a symmetric block protocol in which the transmitter sends encrypted data over the TMDS-like link to the receiver when the receiver is coupled to said TMDS-like link and the receiver decrypts the encrypted data in response to the receiver key and a sequence of count values, wherein the transmitter is configured to generate a pseudo-random value, the transmitter is configured to transmit the pseudo-random value over one of the communication channel and the TMDS-like link to the receiver, and the receiver is configured to include the pseudo-random value as a field of at least one of the count values upon determining that the decrypted result satisfies the predetermined criterion.

76. (currently amended) The receiver ~~system~~ of claim 75, wherein the communication channel is a channel of the TMDS-like link, and wherein the transmitter is configured to transmit the pseudo-random value and the encrypted result over said channel of the TMDS-like link to the receiver when the receiver is coupled to said TMDS-like link.

77. (currently amended) The receiver ~~system~~ of claim 99~~70~~, wherein the system also ~~including:~~ includes an external agent configured to be coupled to each of the receiver and the transmitter, wherein the external agent is configured to provide the transmitter key to the transmitter when coupled to said transmitter and to provide the receiver key to the receiver when coupled to said receiver.

78. (canceled)

79. (currently amended) The method of claim ~~78~~80, wherein step (b) includes the step of determining whether the transmitter key matches the receiver key.

80. (currently amended) ~~The method of claim 78~~ A method for implementing a content protection protocol using a transmitter, a receiver, and a communication link between the transmitter and the receiver, said method including the steps of:

(a) providing a receiver key to the receiver and providing a transmitter key to the transmitter;

(b) operating the transmitter and the receiver to perform a challenge-response procedure to determine whether at least one of the transmitter key and the receiver key satisfies a predetermined criterion, thereby determining whether the receiver key has a predetermined relationship to the transmitter key; and

(c) upon determining that said at least one of the transmitter key and the receiver key satisfies the predetermined criterion, enabling the receiver to use the receiver key to decrypt data received over the link, wherein step (b) includes the steps of:

(d) operating the receiver to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message;

(e) sending the authentication message to the transmitter;

(f) operating the transmitter to perform a predetermined mathematical function on the authentication message to generate a result, and to encrypt the result using the transmitter key to generate an encrypted result;

(g) sending the encrypted result to the receiver;

(h) operating the receiver to generate a decrypted result by decrypting the encrypted result using the receiver key; and

(i) determining from the decrypted result whether said at least one of the transmitter key and the receiver key satisfies the predetermined criterion.

81. (original) The method of claim 80, wherein the transmitter is configured to transmit additional data with the encrypted result to the receiver, said method also including the step of:

(j) upon determining that said at least one of the transmitter key and the receiver key satisfies the predetermined criterion, operating the receiver in response to said additional data.

82. (original) The method of claim 81, wherein the additional data is key material.

83. (original) The method of claim 80, wherein the first data is a pseudo-random value, and step (d) includes the steps of generating the pseudo-random value and encrypting

the pseudo-random value in accordance with the protocol using the receiver key to generate the authentication message.

84. (original) The method of claim 80, wherein the protocol is a symmetric block protocol in accordance with which the transmitter can send encrypted data over the link to the receiver and the receiver can decrypt the encrypted data in response to the receiver key and a sequence of count values, wherein step (b) also includes the steps of:

operating the transmitter to generate a pseudo-random value; and

sending the pseudo-random value to the receiver,

and wherein step (c) includes the step of including the pseudo-random value as a field of at least one of the count values upon determining that said at least one of the transmitter key and the receiver key satisfies the predetermined criterion.

85. (currently amended) The method of claim ~~78~~80, wherein step (c) includes the step of:

preventing the receiver from using the receiver key to decrypt data received over the link unless said at least one of the transmitter key and the receiver key satisfies the predetermined criterion.

86. (currently amended) The method of claim ~~78~~80, wherein step (a) includes the step of:

coupling an external agent to the receiver and sending, from the external agent to the receiver, at least one of the receiver key, an encrypted version of the receiver key, and data enabling the receiver to obtain the receiver key.

87. (currently amended) The method of claim ~~78~~80, wherein the link is a transition minimized differential signaling-like ("TMDS-like") link, and wherein step (a) includes the step of:

coupling an external agent to the receiver and sending, from the external agent to the receiver, at least one of the receiver key, an encrypted version of the receiver key, and data enabling the receiver to obtain the receiver key.

88. (new) A repeater configured to implement a content protection protocol, for use in a communication system including a receiver, at least one transition minimized differential signaling-like ("TMDS-like") link coupled between the repeater and the receiver, a content source, a serial link coupled to the content source, and an external agent configured to be coupled to the receiver and the receiver, wherein the receiver is configured to implement the content protection protocol, is operable in a decryption mode in which it generates decrypted data by decrypting encrypted data using a secret value, the external agent is configured to respond to a ticket request from one of the repeater and the receiver by determining or obtaining a determination as to whether to grant the request, and to send signals to the repeater and the receiver when coupled thereto in response to each granted ticket request to enable the repeater and the receiver to operate respectively in an encryption mode and the decryption mode, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the repeater and the receiver to obtain the secret value, the content source is configured to implement a second content protection protocol according to which the content source generates second encrypted data by encrypting input data using a second secret value and transmits the second encrypted data over the serial link, wherein the repeater includes:

first circuitry configured to be coupled to the at least one TMDS-like link and operable in the encryption mode to generate the encrypted data by encrypting first data using the secret value and transmit the encrypted data over the at least one TMDS-like link; and

second circuitry coupled to the first circuitry and configured to be coupled to be serial link, wherein the second circuitry is configured to implement the second content protection protocol and to be operable in a second decryption mode in which it generates the first data from the second encrypted data including by decrypting the second encrypted data using the second secret value.

89. (new) A transmitter configured to implement a content protection protocol, for use in a communication system including a receiver configured to implement the content protection protocol and operable in a decryption mode in which it generates decrypted data by decrypting encrypted data using a sequence of secret values including a secret value, at least one transition minimized differential signaling-like ("TMDS-like") link coupled to the receiver, and an external agent configured to be coupled to the receiver and to the transmitter, wherein the external agent is configured to respond to a ticket request from one of the transmitter and the receiver by determining or obtaining a determination as to whether to grant the request, and to send signals to the transmitter and the receiver in response to each granted ticket request to enable the transmitter and the receiver to operate respectively in an encryption mode and the decryption mode, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter and the receiver to obtain the secret value, wherein the transmitter includes:

circuitry configured to be coupled to the at least one TMDS-like link and operable in the encryption mode to generate encrypted data by encrypting first data using the sequence of secret values and transmit the encrypted data over the at least one TMDS-like.

90. (new) A router configured to implement a second content protection protocol, for use in a communication system including a transmitter, a receiver configured to implement a first content protection protocol and the second content protection protocol, at least one serial link coupled to the transmitter, at least one additional serial link coupled to the receiver, and an external agent configured to be coupled to at least one of the transmitter, the router, and the receiver, wherein the receiver is configured to generate decrypted data by decrypting encrypted data in accordance with the second content protection protocol using a third secret value, the external agent is configured to respond to response to a ticket request from said at least one of the transmitter, the router, and the receiver by determining or obtaining a determination as to whether to grant the request, and sending signals to at least one of the transmitter, the router, and the receiver in response to each granted ticket request, wherein the signals include at least one of a secret value, a second secret value, the third secret value, an encrypted version of the secret value, an encrypted version of the second secret value, an encrypted version of the third secret value, data enabling the receiver to obtain the secret value, data enabling the router to obtain the second secret value, and data enabling the receiver to obtain the third secret value, wherein the router includes:

circuitry, configured to be coupled to the at least one serial link and the at least one additional serial link and to be operable in a first mode and a second mode, wherein

in the first mode when the circuitry is coupled to the at least one serial link and the at least one additional serial link, the circuitry forwards, from the at least one serial link to the at least one additional serial link, multiply encrypted data received for decryption by the receiver in accordance with the first content protection protocol using the secret value, and

in the second mode when the circuitry is coupled to the at least one serial link and the at least one additional serial link, the circuitry generates encrypted data by performing a translation operation on multiply encrypted data received from the at least one serial link, wherein the translation operation includes decryption of the multiply encrypted data using the second secret value in accordance with the second content protection protocol, and the circuitry forwards the encrypted data to the at least one additional serial link for decryption by the receiver in accordance with the second content protection protocol using the third secret value.

91. (new) A translating router configured to implement a content protection protocol and a second content protection protocol, for use in a communication system including a first link, a transmitter coupled to the first link and configured to implement the content protection protocol to generate encrypted data including by encrypting first data using a secret value and to transmit the encrypted data over the first link, a receiver configured to implement the second content protection protocol, a second link coupled to the receiver, and an external agent configured to be coupled to each of at least two of the receiver, the translating router, and the transmitter, wherein the external controller is configured to perform at least one function essential to implementation of at least one of the content protection protocol and the second content protection protocol, and at least one of the first link and the second link is a transition minimized differential signaling-like ("TMDS-like") link, wherein the translating router includes:

circuitry configured to be coupled to the first link and the second link and operable to generate decrypted data by decrypting the encrypted data using the secret value, to generate translated data by processing the decrypted data, to generate re-encrypted data by encrypting the translated data using a second secret value, and to transmit the re-encrypted data over the second link, to allow the receiver to generate additional decrypted data by decrypting the re-encrypted data using the second secret value.

92. (new) A repeater configured to implement a content protection protocol and a second content protection protocol communication, for use in a communication system including first link, a transmitter coupled to the first link and configured to implement the content protection protocol to generate encrypted data by encrypting first data using a secret value and to transmit the encrypted data over the first link, a receiver configured to implement the second content protection protocol to generate additional decrypted data by decrypting re-encrypted data using a second secret value, a second link coupled to the receiver, and an external agent configured to be coupled to each of at least two of the receiver, the repeater, and the transmitter, wherein at least one of the first link and the second link is a transition minimized differential signaling-like ("TMDS-like") link, and the external agent is configured to perform at least one function essential to implementation of at least one of the content protection protocol and the second content protection protocol, wherein the repeater includes:

circuitry configured to be coupled to the first link and the second link, to generate decrypted data including by decrypting the encrypted data using the secret value, to generate the re-encrypted data including by encrypting the decrypted data using the second secret value, and to transmit the re-encrypted data over the second link.

93. (new) A receiver configured to implement a content protection protocol, for use in a communication system including at least one transition minimized differential signaling-like ("TMDS-like") link, a transmitter coupled to the TMDS-like link and configured to implement the content protection protocol including by operating in an encryption mode to generate encrypted data using a secret value and transmitting the encrypted data over the at least one TMDS-like link, and an external agent configured to be coupled to the receiver and to the transmitter and to respond to a ticket request from one of the transmitter and the receiver by determining or obtaining a determination as to whether to grant the request and sending signals to at least one of the transmitter and the receiver in response to each granted ticket request to enable the transmitter and the receiver to operate respectively in the encryption mode and a decryption mode, wherein the receiver includes:

circuitry configured to be coupled to the TMDS-like link and operable in the decryption mode to generate decrypted data by decrypting the encrypted data using the secret value, wherein the receiver is configured to send the ticket request to the external agent when coupled to the external agent, said ticket request including data indicative of at least one capability of the receiver.

94. (new) A transmitter configured to implement a content protection protocol, for use in a communication system including at least one transition minimized differential signaling-like ("TMDS-like") link, a receiver coupled to the TMDS-like link and configured to implement the content protection protocol including by operating in a decryption mode to decrypt encrypted data received over the TMDS-like link using a secret value to generate decrypted data, and an external agent configured to be coupled to the receiver and to the transmitter and to respond to a ticket request from one of the transmitter and the receiver by determining or obtaining a determination as to whether to grant the request and sending signals to at least one of the transmitter and the receiver in response to each granted ticket request to enable the transmitter and the receiver to operate respectively in an encryption mode and the decryption mode, wherein the transmitter includes:

circuitry configured to be coupled to the TMDS-like link and operable in the encryption mode to generate the encrypted data by encrypting first data using the secret value and to transmit the encrypted data over the at least one TMDS-like link, wherein the transmitter is configured to send the ticket request to the external agent when coupled to the external agent, said ticket request including data indicative of at least one capability of the receiver.

95. (new) The transmitter of claim 94, wherein the data indicative of at least one capability of the receiver indicates whether the receiver can assert unprotected digital data at an output of said receiver.

96. (new) The transmitter of claim 94, wherein the data indicative of at least one capability of the receiver indicates whether the receiver can assert digital data protected by a content protection protocol at an output of said receiver.

97. (new) An external agent for use in a communication system including a transmitter configured to implement a content protection protocol, a receiver configured to implement the content protection protocol, at least one transition minimized differential signaling-like ("TMDS-like") link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data by encrypting first data using a secret value and transmits the encrypted data over the at least one

TMDS-like link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value, wherein

the external agent is configured to be coupled to the receiver and to the transmitter, and to be operable in a mode in which it sends at least one signal to the receiver and at least one additional signal to the transmitter, wherein the at least one additional signal is indicative of at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter to obtain the secret value, and

wherein the at least one signal is indicative of first data and second data, wherein the first data comprise at least one of the secret value, an encrypted version of the secret value, and data enabling the receiver to obtain the secret value, the second data includes a code value that identifies the secret key without revealing the secret key, and the secret key cannot be derived from the second data.

98. (new) An external agent for use in a communication system including a transmitter configured to implement a content protection protocol, a receiver configured to implement the content protection protocol, at least one transition minimized differential signaling-like ("TMDS-like") link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data by encrypting first data using a secret value and transmits the encrypted data over the at least one TMDS-like link to the receiver, the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value, the transmitter is configured to operate in a pass-through mode in response to a control signal, and the receiver is configured to operate in a non-decrypting mode in response to a second control signal, wherein, in the pass-through mode, the transmitter receives data from a source and transmits the data over the at least one TMDS-like link to the receiver without encrypting said data, and in the non-decrypting mode, the receiver does not decrypt any data that it receives from the transmitter over the at least one TMDS-like link, and wherein

the external agent is configured to be coupled to the receiver and to the transmitter, to be operable in a mode in which it sends at least one signal to the receiver and at least one additional signal to the transmitter, wherein the at least one additional signal is indicative of at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter to obtain the secret value, and also to be operable in a second mode in which it sends the control signal to the transmitter and the second control signal to the receiver.

99. (new) A receiver configured to implement a content protection protocol, for use in a communication system also including a transmitter configured to implement the content protection protocol and a communication channel coupled to the transmitter, wherein the content protection protocol includes a procedure for supplying a receiver key to the receiver and a challenge-response procedure for verifying whether the transmitter has a transmitter key matching the receiver key, and the transmitter is configured to perform a predetermined mathematical function on an authentication message received over the channel to generate a result, to encrypt the result using the transmitter key to generate an encrypted result, and to send the encrypted result over the channel, and wherein the receiver includes:

circuitry, configured to be coupled to the communication channel and to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message, to send the authentication message to the transmitter over the channel when coupled to said channel, to generate a decrypted result by decrypting said encrypted result using the receiver key, and to determine whether the decrypted result satisfies a predetermined criterion.

100. (new) A transmitter configured to implement a content protection protocol, for use in a communication system also including a receiver configured to implement the content protection protocol and a communication channel coupled to the receiver, wherein the content protection protocol includes a procedure for supplying a receiver key to the receiver and a challenge-response procedure for verifying whether the transmitter has a transmitter key matching the receiver key, and the receiver is configured to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message, to send the authentication message over the channel, to generate a decrypted result by decrypting an encrypted result received over the channel using the receiver key, and to determine whether the decrypted result satisfies a predetermined criterion, and wherein the transmitter includes:

circuitry, configured to be coupled to the communication channel and to perform a predetermined mathematical function on said authentication message received over the channel to generate a result, to encrypt the result using the transmitter key to generate an encrypted result, and to send the encrypted result to the receiver over the channel when coupled to said channel.

101. (new) The transmitter of claim 100, wherein the circuitry is configured to transmit additional data with the encrypted result over the channel to the receiver when coupled to said channel.

102. (new) The transmitter of claim 101, wherein the additional data is key material.

103. (new) The transmitter of claim 100, wherein the system also includes a transition minimized differential signaling-like ("TMDS-like") link coupled to the receiver, the transmitter is configured to be coupled to the TMDS-like link, the protocol is a symmetric block protocol in accordance with which the receiver decrypts encrypted data received over the TMDS-like link in response to the receiver key and a sequence of count values, the transmitter is configured to send the encrypted data over the TMDS-like link to the receiver when coupled to said TMDS-like link, the transmitter is configured to generate a pseudo-random value and to transmit the pseudo-random value over one of the communication channel and the TMDS-like link to the receiver when coupled to the communication channel and the TMDS-like link, and the receiver is configured to include the pseudo-random value as a field of at least one of the count values upon determining that the decrypted result satisfies the predetermined criterion.

104. (new) The transmitter of claim 103, wherein the communication channel is a channel of the TMDS-like link, and the transmitter is configured to transmit the pseudo-random value and the encrypted result over said channel of the TMDS-like link to the receiver when coupled to said TMDS-like link.